Speech
Interparliamentary Committee meeting:
The reform of the EU Data Protection framework - Building trust in a digital and global world

European Parliament 10 October 2012

Frederik Zuiderveen Borgesius

Ph.D Researcher
Institute for Information Law, University of Amsterdam/New York University
www.ivir.nl/staff/borgesius.html
F.J.ZuiderveenBorgesius[at]uva.nl

Ladies and gentlemen,

Thank you for letting me share my thoughts on the proposals for the Data Protection Regulation. Today I will focus on two points: (i) the definition of "data subject", and (ii) the requirements for consent. First, the definition of "data subject" should be broadened, to emphasize that the Regulation applies to data that can be used to "single out" a person. Second, consent should be taken seriously. Therefore the requirements for consent in the Regulation should be kept like they are.

1. Scope of the Regulation

First: the scope of the definition of the "data subject". The proposed definition is good, but it could be improved by adding the words "or can be singled out".

> Personal data: "any information relating to a data subject" (article 4 (2)).
>
> Data subject: "an identified natural person or a natural person who can be identified, directly or indirectly, **or can be singled out**, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person' (article 4(1)).

The definition of "data subject" is the most important definition of the Regulation, because it sets the scope of the Regulation. If information is outside the scope of this definition, the Regulation does not apply.

For example, some argue that data processing for behavioural targeting falls outside the scope of the data protection regime, if a company does not, or cannot, tie a name to an individual profile. But such nameless profiles can contain highly detailed information about a person.

The profile might include for example which websites a person visits, what she searches for on the web, and which video's she watches on the internet. For users of smart phones, a profile might also include up to date location data. Nameless profiles could also be used to charge a person higher prices in an online shop.[1]

In sum, it's not always relevant whether a company knows the name of a person or not. Moreover, it's often possible to add a name to a nameless profile. Therefore, information that can be used to single out a person, or to distinguish a person within a group, should be within the scope of the Regulation. The idea that data that can be used to "single out" a person are personal data is not new. The Article 29 Working Party has been saying this since 2007.[2]

Apart from adding the phrase on "single out" to the definition of data subject, recital 24 should be amended. Just before the proposal was released in January, the last sentence was added to the recital.[3] This sentence is confusing and should therefore be deleted. The recital thus becomes as follows.

> "When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. ~~It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances~~."

In conclusion, the words "or can be single out" should be added to the definition of "data subject".

---

[1] "Just as it's easy for customers to compare prices on the Internet, so is it easy for companies to track customers' behavior and adjust prices accordingly" (Baker W, Marn M, Zawada C., Price smarter on the Net, Harvard Business Review. 2001 Feb; 79(2):122-7, 157). See generally: J. Turow J, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth* (Yale University Press 2011).

[2] Article 29 Working Party, Opinion 4/2007 on the concept of personal data (WP 136). 20 June 2007; Article 29 Working Party, Opinion 2/2010 on online behavioural advertising (WP 171). 22 June 2010. Many commentators agree with the Working Party. See e.g. Traung P (2010) EU Law on Spyware, Web Bugs, Cookies, etc., Revisited: Article 5 of the Directive on Privacy and Electronic Communications. Bus Law Rev 31:216–228. The American Federal Trade Commission takes a similar position: "The [privacy] framework applies to all commercial entities that collect or use consumer data *that can be reasonably linked to a specific consumer, computer, or other device* (…)" (emphasis added). Federal Trade Commission Report: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (March 2012), www.ftc.gov/os/2012/03/120326privacyreport.pdf, p. 22.

[3] See recital 23 of the proposal version 56 (29 November 2011), http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf.

2. Consent

Consent is the second topic of this talk. Consent should be taken seriously. Silence is not consent. Therefore the conditions for consent in the Regulation should be kept like they are.

If consent would not be taken seriously, the fundamental right to data protection would become hollow. Even sensitive data (regarding for example health or religion) can often be processed on the basis of consent.[4]

Why is the definition of consent important in practice? On the internet consent is often not taken seriously. Some even say that inactivity, or silence, can imply consent.[5] This is wrong under the current Data Protection Directive, because silence is almost never an indication of one's wishes.[6] Likewise, in general contract law, silence almost never constitutes consent.[7] The proposed Regulation correctly emphasises that inactivity is not consent.[8] In sum, the requirements for consent should not be lowered.

Conclusion

To conclude, I hope you remember two points from my speech. First: information that can be used to single out a person should be within the scope of the Regulation. Therefore, the definition of data subject should be amended. Second, consent should be taken seriously. Therefore, the conditions for consent should be kept like they are.

Thank you for your attention. Please feel free to email me if you have any questions.

* * *

[4] See article 9(a) of the proposed Regulation.

[5] "We believe that default web browser settings can amount to 'consent'" (emphasis original). Interactive Advertising Bureau, Response by IAB UK to the Department for Business, Innovation & Skills consultation on implementing the revised EU electronic communications framework (IAB 1 December 2010, www.iabuk.net/sites/default/files/IABUKresponsetoBISconsultationonimplementingtherevisedEUElectronicCommunicationsFramework_7427_0.pdf), p. 2.

[6] The Court of Justice of the European Union confirms that consent cannot easily be assumed (CJEU: Case C-92/09 and C-93/09 *Volker und Markus Schecke GbR* (2010), para 63).

[7] See e.g. article 18(1) of the Vienna Convention on international sale of goods: "A statement made by or other conduct of the offeree indicating assent to an offer is an acceptance. Silence or inactivity does not in itself amount to acceptance." See also article II. 4:204(2) of the Draft Common Frame of Reference (Principles, Definitions and Model Rules of European Private Law): "Silence or inactivity does not in itself amount to acceptance."

[8] See recital 25: "Silence or inactivity should therefore not constitute consent."